REMARKS

Claims 1-11 have been examined, with all claims remaining rejected under 35 USC 103(a) as being unpatentable over Shamir (U.S. Patent No. 5,991,415) in view of Boneh et al. (U.S. Patent No. 6,965,673; hereinafter "Boneh"). Applicant continues to traverse this rejection for the reasons set forth below.

Preliminarily, the Examiner does not specifically state in the Office Action which values of Shamir he equates with the first auxiliary quantity, with the first prime number, with the modulus, with the message, with the second prime number, the second auxiliary quantity, and the result of the exponentiation calculation, as defined in the claims. The Examiner informed Applicant by telephone that he would review the application and then provide Applicant with this information. However, the Examiner never did. **Applicant therefore reasserts a request for interview before a next action in this application to discuss the Examiner's interpretation of the applied references.**

Shamir, in Fig. 2, discloses an exponentiation calculation by means of the Chinese Remainder Theorem. More specifically, box 30 states that the final result is computed by the Chinese Remainder Theorem, and that it is a prerequisite of the Chinese Remainder Theorem that there are two prime numbers p, q, and that there are auxiliary quantities w_1, w_2 (called "S_p, S_q" in the present application). However, w_1, w_2 do not fully correspond to the claimed auxiliary quantities, as explained below.

The claimed invention requires calculating the first auxiliary quantity using the first prime number as the module and using the message; calculating the second auxiliary quantity using the second prime number as the module and using the message.

The Examiner might be comparing these calculating steps to Shamir's box 26, with the first auxiliary quantity being w_1, the second auxiliary quantity w_2 being, the first prime number being p as the modulus in the first calculation, and the second prime number q as the modulus in the second calculation. However, contrary to the claimed invention, box 26 uses the product between j and p as a modulus in the first calculation and uses the product between j and q (note the error in box 26 of Shamir, but the text in column 6 is correct), as the modulus in the second calculation. However, both calculations in box 26 use the expression x, which is included in v_1 and v_2, as determined in block 24.

Therefore, while the claimed first and second steps require the use of the first prime number p, and the second prime number q, as a modulus, Shamir uses the product between the prime number p and the random integer j as a modulus, and uses the product between random number j and prime number q as a modulus. Since j is multiplied by p and q, the result, that is the product between j and p or the product between j and q, is not a prime number, but is non-prime. Thus, Shamir does not suggest the first prime number used as the modulus and the second prime number used as the modulus.

The Examiner might be considering the claimed combining step to correspond to box 30 of Shamir, since the "final result" in Shamir, box 30, corresponds to the "result of the exponentiation calculation." However, the final result which is computed by box 30 is never verified, that is compared to anything or processed by anything, etc. Shamir does not disclose verifying, and consequently, also does not disclose suppressing an output if the verifying step shows that the verifying algorithm provides a result other than the predetermined result, as also required by the claimed invention.

Regarding the combining step, the Examiner wrongly states that Shamir's box 26 corresponds to the combining step.

Applicant questions as to what "combined" in Shamir's box 26 means, in order to obtain a result of the exponentiation calculation. Neither w_1 nor w_2 is the "result" of the exponentiation calculation. If the Examiner were to consider the first three lines of claim 1, i.e., that the exponentiation calculation is done by means of the Chinese Remainder Theorem, then he would not have thought of stating that the combining step 26 results in any exponentiation calculation.

Possibly, however, the Examiner might believe that the calculation v_1 corresponds to the claimed first calculating step, and that v_1 is the claimed "first auxiliary quantity." The Examiner might further believe that d_1 (mod j*p) corresponds to the claimed second calculating step and is the claimed "second auxiliary quantity." Then the first line in box 26 might indeed be a combination of two quantities.

However, the Examiner's reading in this regard is contrary to the definitions in claim 1 for the following reasons:

v_1 is equal to x (mod j*p) as defined in block 24. And, x is the expression which corresponds to the first auxiliary quantity having to be calculated using the first prime number as the modulus, as required by the claimed invention. But again the modulus is not the prime number p, but is the product between j and the prime number p, and as is known, a product between a number and a prime number is <u>never</u> again a prime number. Therefore, this reading does not meet the limitation in accordance with claim 1 that the first auxiliary quantity has to be calculated using the first prime number as the modulus.

Regarding the second auxiliary quantity, this situation is similar. d_1 (mod j*p) is equal to d (mod phi (j*p)) (mod j*p). This calculation includes two moduli, but none of the moduli is a prime number. Furthermore, it is clear that d is the secret exponent and that d_1 is a quantity derived from the secret exponent. In this calculation, which the Examiner compares to the "second auxiliary quantity," the message does not occur. Thus, the only combination which takes place in block 26 is between two quantities v_1 and d_1 (mod j*p), where neither the first prime number nor the second prime number is used as a modulus, and where the message is not used in the calculation of the figure which the Examiner considers to be the "second auxiliary quantity."

Apart from this, saying that w_1 or w_2 might correspond to the "result" of the exponentiation calculation, or saying that v_1 on the one hand and d_1 (mod j*p) on the other hand, correspond to the "first auxiliary quantity" and "second auxiliary quantity," as required in the claimed invention for the usage of the Chinese Remainder Theorem, is also contrary to the claimed limitations.

Thus, the only technically useful reading of Shamir would be to say that w_1 corresponds to the "first auxiliary quantity" that w_2 corresponds to the "second auxiliary quantity," since only under this interpretation, both auxiliary quantities are calculated using the message, although as outlined above, the moduli are not prime numbers in Shamir and are, specifically, not the specific prime numbers p, q, which are decisive in the Chinese Remainder Theorem, since p, q is equal to the modulus N.

Therefore, in response to section 3.1 of the Office Action, box 26 is not a combining step as claimed, since the claimed combining step, in the end, obtains the result of the exponentiation calculation which is then used in the subsequent verifying step for verification purposes. This is definitely not the case, since there is no output from box 30 in Shamir, which is used for any further verification.

On page 5 of the Office Action, the Examiner states that Shamir is silent regarding the first calculating step and the second calculating step. However, the Examiner did not state where in Boneh he believes these two calculating steps to be located. He firstly points to column 5, lines 6-10, but there is not any calculating steps disclosed. Applicant does not see any first auxiliary quantity, a first prime number, or a message or a modulus, etc. Therefore, this passage does not help in stating that these two calculating steps are disclosed in Boneh.

Then, the Examiner points to column 7, lines 53-57. This passage only says that there is a modulus N and the modulus has factors p, q, which are indeed prime numbers, but again, Applicant does not see any indication of an auxiliary quantity or a calculation using these prime numbers as moduli and using the message as specifically defined in detail in the first calculating step and the second calculating step as claimed.

In column 7, lines 50-52, there is even a calculation E indicated which uses the modulus N, rather than the prime numbers and which, specifically, is completely done without any auxiliary quantities.

Furthermore, the Examiner points to column 4, lines 58-65, where the Chinese Remainder Theorem and Rabin's Signature Scheme are mentioned, but again, Applicant does not see anything regarding the first calculating step and the second calculating step.

Furthermore, Boneh does not disclose any feature corresponding to the claimed verifying step, and the Examiner does also not assert this.

Moreover, the Examiner also does not state anything regarding the suppression of an output, as also claimed.

Regarding section 3.2, the Examiner repeats these arguments and cites column 4, lines 50-67, of Shamir. The Examiner possibly intended to argue that one can combine both references. However, one cannot combine these Shamir and Boneh. Importantly, however, even when the Examiner combines these references, the combination still does not show any of the following limitations: the first calculating step; the second calculating step; or the combining step. Importantly, none of the references discloses that, following the combining step, the result of the exponentiation calculation is verified.

In contrast to Shamir where any "pre-results or intermediate values" are used for verifying, the present invention is unique in that the result of the exponentiation calculation after the combination step is verified. This feature is specifically useful and technically important since any fault attacks against the final combination step are detectable, while this is not the case in Shamir. Consider, for example, that an attacker manages to attack the calculations in block 30, while he did not introduce any errors into the calculations in blocks 20, 24, 26, 28, such a fault attack would not be detected in Shamir with the result that the whole cryptographic security in Shamir would be broken. In accordance with the present invention, on the other hand, the security verification is done after the critical combination step, so that any fault attacks introduced not only during a pre-computation, but also even introduced during the combination step, would be detected. Therefore, the attacker would have a chance to break Shamir by specifically introducing a fault attack into the calculations in block 30 of Fig. 2 of Boneh. He would, however, not have a chance to break the present invention's cryptographic device, due to the fact that the attack against the computations in block 30 would have been detected due to the fact that the result of the exponentiation calculation is verified in accordance with the verifying step of the claimed invention.

Thus, the claims are patentable over the applied references for at least these reasons.

With further regard to dependent claim 6, it is clear that "s" is the final result of the combining step, and the verification algorithm includes calculating s mod p and s mod q. Thus when s mod p = sp as defined in the first equation of claim 6, then no fault attack occurred. On the other hand, when this equality, as defined in the last paragraph of claim 1, is not fulfilled, then there was a fault attack and the output of the erroneous calculation is suppressed in order to defend against the attack.

The final result of the Chinese Remainder Theorem in block 30 of Shamir, which could be argued to correspond to "s" in claim 6, is never used for performing calculations comparable to the last lines of claim 6. Therefore, claim 6 is patentable over the applied references for these additional reasons.

In view of the above amendment, Applicant believes the pending application is in condition for allowance.

In the event a fee is required or if any additional fee during the prosecution of this application is not paid, the Patent Office is authorized to charge the underpayment to Deposit Account No. 50-2215.

Dated: May 21, 2008

Respectfully submitted,

By Laura C. Brutman

Laura C. Brutman
Registration No.: 38,395
DICKSTEIN SHAPIRO LLP
1177 Avenue of the Americas
New York, New York 10036-2714
(212) 277-6500
Attorney for Applicant